QA Deliverable: Login and MFA Testing

1. Manual Testing Test Plan

1.1 - Test the login page with various input combinations (valid and invalid credentials)

1.1.1 Valid Input: Correct username and correct password combination lead to navigation to the MFA page.

1.1.2 Invalid Inputs:

- Valid username and invalid password should lead to error (specific, not generic).
- Invalid username and valid password should lead to error (specific, not generic).
- Nonexistent credentials should lead to error (specific, not generic).
- Empty username and valid password should lead to a validation error/message (specific, not generic).
- Valid username and empty password should lead to a validation error/message (specific, not generic).
- If both inputs are empty, it should lead to a validation error/message and Login button should be disabled (specific error message, not generic).
- Incorrect format for any of the two inputs should create a validation error/message with specific text as to what went wrong (specific, not generic).

1.1.3 Edge cases:

- All caps for Username and/or Password inputs should fail with appropriate validation error/message (if the credentials format demands it).
- No caps inputs should fail with appropriate validation error/message (if the credentials format demands it).
- Leading and/or trailing spaces should fail with appropriate validation error/message (in theory they should be filtered out or a specific validation message should show up).
- Underscores, punctuation, or special characters should fail or succeed according to format specifications (with specific error message).
- Numbers in username and/or password inputs according to format specifications (if they are not allowed an appropriate validation message should appear).

- Empty string for both Username and Password inputs (activates guard on Login page).
- Space counting as a valid character in the string for both Username and Password inputs (a validation message should indicate as such).
- Extremely long/short input, for testing max and min validation length.
- Incorrect format in general according to specifications.
- Masking characters for password and/or username input.
- Login button should be disabled unless both inputs are valid and not empty, or validation message should indicate as such (“Please fill out this field”, “This field is required”, etc.). (UI/UX)
- Check label structure, display and appearance. (UI/UX)
- ARIA (Accessible Rich Internet Applications)/screen reader support. (A file with similar name is attached to the folder as to what can be included). (UI/UX)
- Accessibility: Error messages visible, aligned, not overlapping, screen size, zooming in/out. (UI/UX)
- After failing login, a Retry button should be visible or a back to login form, accordingly. (Navigation/Behavior)
- Check if the Refresh button clears input values. (Navigation/Behavior/Security)
- Check if the Back navigation after (failed) login clears or retains input values. (Navigation/Behavior/Security)
- Check if password autofill/autosave restrictions exist.
- Maximum retry limit to check if user gets blocked or locked out.

1.2 - Test the MFA step with correct and incorrect MFA codes.

1.2.1 Valid Input: Correct MFA Code redirects to dashboard page.

1.2.2 Invalid Inputs: Wrong MFA Code redirects to error page.

- Empty input should trigger a validation error.
- Space-only input should trigger a validation error.
- Non-digit input (letters, special characters, symbols etc. The format should be specified and valid/invalid inputs tested accordingly).

1.2.3 Edge cases:

- MFA retry limit.
- Expired MFA.
- Check if navigating back retains or clears input value.
- Check if the Refresh button retains/clears input value.
- Direct unauthorized access to the MFA page (without login).

- Verification button should become disabled if format/length etc. is not valid or if input is not entered.
- Add an expired/reused MFA code.

1.3 - Test the navigation to an authenticated page that requires a valid session cookie

1.3.1 Happy Path: Successful login and correct MFA code redirect to dashboard page.

1.3.2 Unauthorized cases:

- Missing cookie: Open to /dashboard directly (in incognito) should lead to Unauthorized page.
- Invalid cookie: Manually invalid cookie should lead to Unauthorized page.
- Valid cookie: Manually valid cookie should lead to redirection to /dashboard page.

1.3.3 Edge cases:

- Session timeout**.**
- After logging out, navigating back should not display dashboard (security issue).
- Refreshing page while still on the Dashboard page remains authenticated.
- Navigating directly from the MFA page to the Dashboard page without valid cookie should fail.

1.4 General test/edge cases

- 404 / broken URL/incorrect URL should show error.
- “Remember Me” option (not implemented).
- Password reset / Sign up / Help links (not implemented).
- “Clear all inputs” button (not implemented).
- Verify layout in different browsers (verified for Edge and Chrome).
- Responsive check on mobile vs desktop resolutions for all pages.
- Very small / very large screen sizes, zoom in/out for all pages.
- Implement Navigate Back/Retry button for invalid logins (within valid retry limits).

Side note: Vulnerabilities after npm install (occurred while running/setting up the application, not an error)

- When you see:
  npm install
  found X vulnerabilities (Y low, Z high, etc.)
  If this is just for local testing/QA purposes, it is usually safe to ignore.
  If preparing for production:
  Run npm audit to see details.
  Run npm audit fix to auto-fix if safe.
  If unresolved, consider manual dependency update or patch.
  Since this is a demo test app, vulnerabilities don't necessarily need fixing, but in a real-world project at least a review would be needed.

1.5 Bugs found

1.5.1 Validation messages are missing (in general), specific messages should be added for possible cases. The generic page that is shown is not helpful for the user to understand what went wrong and retry.
- Examples: “This field is required.”, “Invalid format.”, “Minimum length should be X characters long.”, “The format of the input should contain lower characters and at least one number and special character”, etc.

1.5.2 Min/Max length validation for inputs is missing.
- Steps to reproduce: Try out different lengths of the input(s) such as 1 (minimum), 10, 100, 256 (usually max length). Expected result: A specific validation message appears. Actual result: No validation message.

1.5.3 Space-only strings are allowed.
- Steps to reproduce: Enter a space-only string (however long, one should suffice). Expected result: A specific validation message appears. Actual result: No validation message.

1.5.4 MFA expiration time limit is missing.

1.5.5 Session timeout is missing.

1.5.6 Toast messages with specified details are missing (session timeout etc.).

1.5.7 All/No caps validation for Username and Password is missing.

1.5.8 Special character validation is missing.

1.5.9 Username and Password format information is missing. (could be displayed with validation messages) This includes almost all of the previous bugs, since the testing cases would me more specific.

1.5.10 Validation that both Username and Password inputs are required is missing. (default message appears on screen, this is an alternative suggestion)

1.5.11 Navigation to previous page (Back) retains input values, this behavior should not be valid.
1.5.12 Directly navigating to the MFA page is allowed (without login) while it should display an unauthorized message.
1.5.13 In general, if the format of the inputs (Username, Password, MFA Code) is not valid, the correct page is loaded (Incorrect credentials), but there is no specific information for the user so they can better understand what went wrong.
1.5.14 Maximum retry limit on both the login page and the MFA Code page until user is blocked.

1.6 Improvements

- Add min/max length validation for inputs.
- Disallow spaces-only strings.
- Add retry limits for login & MFA.
- Add MFA expiration (time-based).
- Prevent direct MFA access without valid login.
- Implement logout endpoint.
- Add session timeout.
- Add forgot password / sign up / help links.
- Add “Remember me” option
- The correct/valid format of the credentials should be provided/displayed (this could be displayed in a Sign-up page, as the user types in the values).
- Standardize error messages (clear, consistent).
- Session time out handling.
- Expired MFA code time limit.
- Define non allowed characters when typing in credential values (specifically for leading and trailing spaces, as well as a full entry of just spaces).